

Claim 1 recites three separate encryption keys, a package encryption key, an escrow encryption key, and the addressee's public key. The package encryption key is used by the sender to encrypt the package, i.e., the document to be sent. The sender then contacts the server and receives an escrow encryption key for encrypting the package key. This allows the server to decrypt the package encryption key and re-encrypt the package decryption key using the recipient's generated public key. In this way, the package is fully secure from being read by any party until the intended recipient decrypts the package.

By contrast Smith merely shows a sender holding a package until an intermediate system contacts a recipient and generates a private public key pair for the recipient and returns the public key to the sender. The sender is unable to send the package until the recipient sends the public key.

This is the exact problem solved by the current system is that the package can be stored in escrow, away from the sender, yet secure until the package has been sent to the recipient. The package is initially sent with a "package" encryption, and sent to the recipient using the public key. The decryption of the package key and re-encryption using the public key by the intermediate storage server is facilitated by the encryption key.

The Examiner cites Smith as teaching a "package encryption key" at Col 5, lines 38-65, however, this is clearly only the recipient public key. The Examiner cites Smith as teaching a "package decryption key encrypted with an escrow key" at Col. 5, lines 30-37, however, this is nowhere shown. The Smith patent merely shows generating a public and private key for the recipient. The Smith patent does not show storing the package in escrow, but instead sends the file as soon as the package has been encrypted using the only key available, i.e., the recipient public key. See Col. 7, lines 1-9. The Examiner cites

Smith as shown obtaining a new key and decrypting the package key and re-encrypting with the public key. This is nowhere shown as only one key is disclosed in the Smith patent, and therefore there would be no reason to decrypt and re-encrypt with the same key. The Examiner also cites Smith as showing "transmitting to the addressee the package decryption key encrypted with the addressee's new public key." However, Smith only shows sending a document encrypted with the recipient's public key, and the recipient already has the private key so there is no reason, and in fact should be discouraged from, sending the private key via e-mail to the recipient. As shown in Col. 7, line 3-6 "indicates that the document 12 can now be encrypted with the public key.... The *encrypted document 70* is then delivered to the recipient." (emphasis added) Nowhere does it suggest that the key to decrypt the document is sent.

The use of the package encryption key allows the document to be stored in escrow while secure from alteration or viewing by third parties. The Examiner suggests that the second encryption will make the document more secure, however, if the document is not stored in escrow the document will not be "more secure" than if it was still under the initial encryption. And since Smith only shows one encryption, there is no "re-encryption". Further deliveries to the recipient would not "re-encrypt" the same package, and both the current system and the Smith system envision using the same recipient public key each time a package is sent to the recipient, so there is no reason to change the key as cited by the Examiner as a rationale for re-encryption. The only possible reason for re-encryption using the third key (i.e., the recipient public key) is impermissible hindsight using the process described by the present application to facilitate escrow storage of an encrypted document. It is therefore respectfully submitted that claim 1 is allowable over the art of record. The two remaining independent claims, namely, claims 11 and 18 each recite the

three encryption keys for serving the same functions as described above and should therefore be allowable for at least the same reasons. The remaining claims depend from claims 1, 11 and 18 and should be allowable for at least the same reasons.

Formal Drawings

Formal drawings were filed with the application on June 14, 2001. A review of the Office Action has failed to uncover whether the drawings were accepted by the Official Draftsman or whether a Form 948 rejection was issued by the Official Draftsman. An indication of the status of the drawings is respectfully requested with the next communication from the Patent Office.

Summary

Applicants have made a diligent and bona fide effort to answer each and every ground for rejection or objection to the specification including the claims and to place the application in condition for final disposition. Reconsideration and further examination is respectfully requested, and for the foregoing reasons, Applicant respectfully submits that this application is in condition to be passed to issue and such action is earnestly solicited. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Robert N. Blackmon, Applicants' Attorney at 703-684-5633 to satisfactorily conclude the prosecution of this application.

Dated: September 26, 2005

Respectfully submitted,



Robert N. Blackmon
Reg. No. 39494
Attorney/Agent for Applicant(s)

Merek, Blackmon & Voorhees, LLC
673 S. Washington St.
Alexandria, Virginia 22314
Tel. 703-684-5633
Fax. 703-684-5637
E-mail: RNB@MBV-IP.com